AAECC (2008) 19:349–363
DOI 10.1007/s00200-008-0078-9

Computation of the weight distribution of CRC codes

Felice Manganiello

Received: 13 July 2006 / Revised: 7 April 2008 / Published online: 9 May 2008

Abstract In this article, we illustrate an algorithm for the computation of the weight distribution of CRC codes. The recursive structure of CRC codes will give us an iterative way to compute the weight distribution of their dual codes starting from some "representative" words. Thanks to MacWilliams' Theorem, the computation of the weight distribution of the dual codes can be easily brought back to that of CRC codes.

Keywords CRC codes · Distance · Linear recurring sequences · Polynomial ring · Weight distribution

1 Introduction

Cyclic Redundancy Check (CRC) codes are an important class of error detecting codes. These codes are widely used in computer communication networks because of their easy and fast encoder and decoder implementation and their considerable burst-error detection capability. These properties are provided by the structure of shortened cyclic codes. The capability to detect burst-errors is discussed in [8].

To measure the degree of goodness of error-detecting codes, we have to investigate two properties: the *minimum distance* and the *undetected error probability* (P_{ue}). The performance of the code improves when the minimum distance increases or when P_{ue} decreases.

To investigate these two properties, it is important to know the *weight distribution* of the code. A way to compute this distribution is by computing the weights of the

The author was partially supported by the Swiss National Science Foundation under Grant no. 113251.

F. Manganiello (✉)
Universität Zürich, Institut für Mathematik, Winterthurerstr. 190, 8057 Zürich, Switzerland
e-mail: felice.manganiello@math.uzh.ch

codewords of the dual code. The weight distribution of the code itself is then provided by MacWilliams' Theorem [6].

In the late 1980s Fujiwara, Kasami and Lin [2] provided a method to compute the minimum distance of Hamming codes. In the early 1990s the method was extended to any CRC code over the binary field. The structure of CRC codes offers the opportunity to construct an ad hoc algorithm that has low computational cost [1]. This work mainly extends the algorithm of [1] to CRC codes over any finite fields.

Another method using Gröbner Bases can be found in [7].

The sections are organized as follows. The second section of this paper is concerned with preliminary notions about CRC codes and properties they have in common with cyclic codes.

The third section deals with the fundamental step of the algorithm. We examine the connection between Linear Recurring Sequences (LRS's) and the words of the dual code of a CRC code, explain the need of choosing the best LRS's, and consider the bijective relation between LRS's and elements of $\mathbb{F}_q[x]/(g(x))$, where $g(x)$ is the polynomial generating the code.

We then turn to studying the structure of the ring $\mathbb{F}_q[x]/(g(x))$. The fourth section shows that it is possible to use the *Chinese Remainder Theorem* while working with quotient rings via powers of irreducible polynomials.

The main task of the fifth section is to find representatives of the x-orbits in the ring $\mathbb{F}_q[x]/(g(x)^t)$, where $g(x)$ is an irreducible polynomial.

We then give a pseudocode representation of the algorithm in the sixth section. We end in the seventh section with the study of the complexity of the algorithm.

2 Preliminaries

Definition 1 Let $n, r \in \mathbb{N}$ with $n > r > 0$. Let $q \in \mathbb{N}$ be some power of a prime number p and $g(x) \in \mathbb{F}_q[x]$ a monic polynomial such that $\deg g(x) = r$ and $g(0) \neq 0$. An $(n, n-r)$ CRC code C is the set

$$C = \left\{ c(x) \in \mathbb{F}_q[x] \mid c(x) = g(x)m(x),\ \deg m(x) < n - r \right\}.$$

Notice that a CRC code is cyclic if and only if the generator polynomial $g(x)$ divides $x^n - 1$.

From this representation, it is easy to deduce that CRC codes are shortened cyclic codes. In fact, a basis of a CRC code can be formed by x-multiplications of the generator polynomial.

Recall that given a polynomial $g(x)$, the dual code of a CRC code of any length generated by $g(x)$ is in bijection with the ring $\mathbb{F}_q[x]/(g(x))$.

2.1 Notations

In this work, we will use the following notations:

- $\mathbb{F}_q$ will be a finite field of characteristic p, $q = p^\delta$ for some $\delta \in \mathbb{N}_+$;
- $n \in \mathbb{N}_+$ will be the length of the CRC code;

- $g(x) \in \mathbb{F}_q[x]$ will be the monic generator polynomial of a CRC code, with $g(0) \neq 0$, $\deg g(x) = r$ and $0 < r < n$;
- $g(x) = \prod_{i=l}^{m} g_l(x)^{e_l}$ will be the irreducible decomposition of $g(x)$ over $\mathbb{F}_q$;
- $u(x)$ will denote both an element of the ring $\mathbb{F}_q[x]/(g(x))$ and a polynomial of $\mathbb{F}_q[x]$;
- $\mathcal{R}_g^q$ will be the ring $\mathbb{F}_q[x]/(g(x))$ and $\mathcal{R}_{g^t}^q$ the ring $\mathbb{F}_q[x]/(g(x)^t)$;
- M_g^q will be the multiplicative group of $\mathcal{R}_g^q$, i.e. $\left(\mathbb{F}_q[x]/(g(x))\right)^*$, and $M_{g^t}^q$ the multiplicative group of the ring $\mathcal{R}_{g^t}^q$.

3 Quotient ring by a primitive polynomial and fundamental step of the algorithm

In this section the fundamental step of the algorithm will be illustrated.

The next theorem is part of Theorem 6.40 of [4]. As a matter of historical interest this result can be found in [3].

Theorem 2 *Let $u(x) \in \mathbb{F}_q[x]$ be a polynomial with $\deg u(x) < \deg g(x)$. Then there exists exactly one sequence $(c_i)_{i\in\mathbb{N}} \subset \mathbb{F}_q^{\mathbb{N}}$ such that*

$$\frac{u(x)}{g(x)} = \sum_{i=0}^{\infty} \frac{c_i}{x^{i+1}} =: c(1/x).$$

Moreover the sequence $(c_i)_{i\in\mathbb{N}}$ satisfies the linear relation

$$c_i = -g_0 c_{i-r} - \cdots - g_{r-1} c_{i-1}, \quad i \geq r. \tag{1}$$

As an immediate application one obtains the following corollary.

Corollary 3 *There exists a bijection between the ring $\mathcal{R}_g^q$ and the set of all LRS's with characteristic polynomial $g(x)$.*

It follows that there is a bijection between the set of LRS's with characteristic polynomial $g(x)$ and the dual code of any CRC code whose generator polynomial is $g(x)$. In the following theorem, we make this bijection explicit.

Theorem 4 *Let L_g be the set of all LRS's over $\mathbb{F}_q$ with characteristic polynomial $g(x)$. Let C be an $(n, n-r)$ CRC code over $\mathbb{F}_q$ whose generator polynomial is $g(x)$, and $C^\perp$ its dual code. Then the following relation*

$$\begin{aligned} \psi : \quad L_g &\to C^\perp \\ (c_i)_{i\in\mathbb{N}} &\mapsto (c_0, \ldots, c_{n-1}) \end{aligned}$$

is bijective.

This bijection allows one to work with LRS's rather than with words of the dual code. The next lemma will allow us to reduce the number of LRS's that we work with.

Lemma 5 *Let $C \subset \mathbb{F}_q^n$ be a CRC code with generator polynomial $g(x)$, and $(c_i)_{i\in\mathbb{N}} \in L_g$. Then*

$$(c_k, \ldots, c_{k+n-1}) \in C^{\perp} \quad \forall\, k \in \mathbb{N}.$$

With this Lemma one can "extract" words of the dual code from a LRS.

We now describe a good way to construct a LRS.

Let $u(x) \in F_q[x]$ be such that $\deg u(x) < \deg g(x)$. Then

$$\frac{u(x)}{g(x)} = \frac{u_{r-1}}{x} + \frac{u'(x)}{xg(x)}, \tag{2}$$

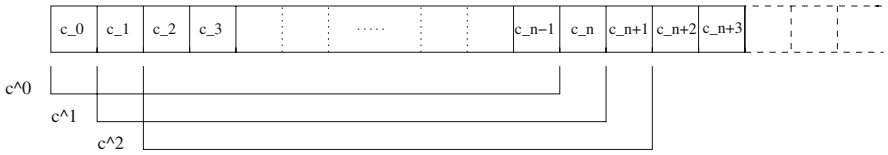
where u_{r-1} is the x^{r-1} coefficient of $u(x)$ and $u'(x) = xu(x) - u_{r-1}g(x) \equiv xu(x) \pmod{g(x)}$. It is trivial to see that the polynomial $u'(x)$ satisfies the condition on the degree. Relation (2) can be iterated, and the resulting sequence of the extracted coefficients u_{r-1} is a LRS.

As an aside, note that LRS's can be easily constructed using a Linear Feedback Shift Register (LFSR) with generator polynomial $g(x)$.

3.1 The fundamental step

This subsection follows the lines of [1]. We repeat the argument here for the sake of completeness.

Let us consider a LRS $(c_i)_{i\in\mathbb{N}}$ with characteristic polynomial $g(x)$. The following figure depicts the idea of the algorithm; this scheme follows from Lemma 5.



In the figure above, $c^{(k)} \subset \mathbb{F}_q^n$ denotes the k-th word of the dual code extracted from the above sequence.

The figure leads directly to relations between the weight distribution of the words thus extracted:

Remark 1 (Weight relations between words)

- if $c_k \neq 0$ and $c_{k+n} = 0$, then $wt(c^{(k+1)}) = wt(c^{(k)}) - 1$;
- if $c_k = 0$ and $c_{k+n} \neq 0$, then $wt(c^{(k+1)}) = wt(c^{(k)}) + 1$;
- $wt(c^{(k+1)}) = wt(c^{(k)})$ otherwise.

This remark will be very useful in decreasing the computational cost of the algorithm. Once the weight of the first extracted word has been computed, the weights of the following words can be easily determined. This procedure has a minimal computational cost, because the operations of addition or subtraction are of constant time complexity.

A way to compute all the weights of $C^{\perp}$ from just two LFSR's is explained in [1].

3.2 Relation between LRS's and words of $C^{\perp}$

Now we are able to extract words of the dual code from LRS's, but some questions are still unanswered. What is a minimal set of LRS's sufficient to determine the weight distribution? How can we be sure that we are not considering the same word more than once?

Definition 6 Let $u(x) \in \mathbb{F}_q[x]$ with $\deg u(x) < \deg g(x)$, and $(c_i)_{i\in\mathbb{N}} \subset \mathbb{F}_q^{\mathbb{N}}$ be the LRS related to $u(x)$ as in (2). We denote by $C_u^{\perp} \subset C^{\perp}$ the set of all codewords extracted from $(c_i)_{i\in\mathbb{N}}$.
The order of $u(x)$ is the least natural number o_u such that $u(x)$ divides $x^{o_u} - 1$.

Lemma 7 *Let $u(x) \in \mathbb{F}_q[x]$ such that $\deg u(x) < \deg g(x)$. The cardinality of $C_u^{\perp}$ is*

$$|C_u^{\perp}| = ord\left(\frac{g(x)}{\gcd(g(x), u(x))}\right).$$

The proof follows directly from the relation between the number of words that can be extracted, the period of $(c_i)_{i\in\mathbb{N}}$ and the definition of the *order* of a polynomial. Details can be found in [1].

3.3 x-orbits, LRS's and Words of $C^{\perp}$

Notation For $u(x) \in \mathcal{R}_g^q$, we denote by $\mathfrak{C}_u^{\perp}$ the x-orbit of $u(x)$.

It is well known that x-orbits can be considered as equivalence classes in the ring $\mathcal{R}_g^q$. The next lemma gives an explicit relation between the x-orbits and the sets $C_u^{\perp}$.

Lemma 8 *Let $u_1(x), u_2(x)$ be two distinct elements of $\mathcal{R}_g^q$. Then*

$$u_2(x) \in \mathfrak{C}_{u_1}^{\perp} \iff C_{u_1}^{\perp} = C_{u_2}^{\perp}.$$

It follows from the previous lemma that the dual code can be constructed by taking the union of disjoint sets that are related to the x-orbits of the ring $\mathcal{R}_g^q$. These orbits are also related to LRS's. Our goal is to find a representative for each x-orbit. Thereafter, using the *fundamental step*, we will be able to compute the weight distribution of the dual code.

4 Application of the Chinese Remainder Theorem

We now want to obtain a representation of the structure of the ring $\mathcal{R}_g^q$ that will be useful for our particular algorithm. We will look for a decomposition of the ring into x-orbits.

From the Chinese Remainder Theorem we know that

$$\mathcal{R}_g^q \cong \prod_{l=1}^{m} \mathcal{R}_{g_l^{e_l}}^q, \tag{3}$$

where $g(x) = \prod_{l=1}^{m} g_l(x)^{e_l}$ is the irreducible factor decomposition.

Let us write the isomorphism explicitly in our case. The following theorem is claimed implicitly in [1].

Theorem 9 *Let $g(x) \in \mathbb{F}_q[x]$ be a monic polynomial such that $g(0) \neq 0$ with the irreducible decomposition just above.*

The map

$$\phi : \mathcal{R}_g^q \to \prod_{l=1}^{m} \mathcal{R}_{g_l^{e_l}}^q$$

given by $\phi(u) = (u_1, \ldots, u_m)$ with

$$u_l(x) \equiv u(x) \pmod{g_l(x)^{e_l}}$$

is an isomorphism with inverse

$$\phi^{-1}(u_1, \ldots, u_m) = \sum_{l=1}^{m} u_l(x) v_l(x) \frac{g(x)}{g_l(x)^{e_l}} \pmod{g(x)},$$

where $v_l(x)$ is the multiplicative inverse of $g(x)/g_l(x)^{e_l}$ in $\mathcal{R}_{g_l^{e_l}}^q$.

Let u_l be an element of the ring $\mathcal{R}_{g_l^{e_l}}^q$, we will denote by $u_l^{(k_l)}$ the equivalence class of $x^{k_l} u_l$. From the paper [1] and some calculations, one obtains the next theorem.

Theorem 10 *Let $g(x) \in \mathbb{F}_q[x]$ be monic with $g(0) \neq 0$ and $g(x) = \prod_{l=1}^{m} g_l(x)^{e_l}$ be its irreducible decomposition. Let $\mathfrak{C}_{u_l}^{\perp}$ be x-orbit of $\mathcal{R}_{g_l^{e_l}}^q$ with cardinality d_l and representative u_l, $l = 1, \ldots, m$.*

A complete set of representatives for the x-orbits of $\mathcal{R}_g^q$ is given by

$$\left(u_1, u_2^{(k_2)}, \ldots, u_m^{(k_m)}\right) \in \prod_{l=1}^{m} \mathcal{R}_{g_l^{e_l}}^q$$

for $0 \leq k_l < \gcd(d_l, \operatorname{lcm}(d_1, \ldots, d_{l-1}))$, $l = 2, \ldots, m$.

5 Decomposition of $\mathcal{R}^q_{g^t}$ into x-orbits

Let t be a natural number and $g(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree r. Then

Lemma 11 *Every $f(x) \in \mathcal{R}^q_{g^t}$ can be represented uniquely as*

$$f(x) = \sum_{l=0}^{t-1} f_l(x) g(x)^l,$$

where $f_l(x) \in \mathbb{F}_q[x]$ and $\deg f_l(x) < \deg g(x)$.

The next step is to investigate subsets of the ring $\mathcal{R}^q_{g^t}$ which are closed under x-multiplication.

Theorem 12 *Let $u(x) \in \mathcal{R}^q_{g^t}$, $l_u := \max\left\{i \in \mathbb{N} \mid g(x)^i | u(x)\right\}$ be the representative of minimal degree of a class $u(x) \in \mathcal{R}^q_{g^t}$, and $\bar{u}(x)$ the factor of $u(x)$ coprime with $g(x)$. The following are equivalent:*

1. $u'(x) \in \mathfrak{C}_u^{\perp} \subset \mathcal{R}^q_{g^t}$,
2. $l_{u'} = l_u$ *and* $\bar{u}'(x) \in \mathfrak{C}_{\bar{u}}^{\perp} \subset \mathcal{R}^q_{g^{t-s}}$.

The proof of this theorem is an easy computation.

Remark 2 Remarks from the theorem.

1. The maximal power of $g(x)$ that divides an element of the x-orbit $\mathfrak{C}_u^{\perp}$ does not depend on the choice of element;
2. The choice of the best representative of x-orbits can be limited to the set of elements of $\mathcal{R}^q_{g^t}$ whose representatives in $\mathbb{F}_q[x]$ are coprime with $g(x)$.

The next corollary follows from Lemma 11 and the previous theorem.

Corollary 13 *The ring $\mathcal{R}^q_{g^t}$ can be decomposed as follows:*

$$\mathcal{R}^q_{g^t} = \{0\} \cup \bigsqcup_{l=0}^{t-1} g(x)^l \cdot M^q_{g^{t-l}},$$

where the sets

$$g(x)^l \cdot M^q_{g^{t-l}} = \left\{u(x) \in \mathcal{R}^q_{g^t} \mid u(x) = g(x)^l \bar{u}(x),\ \bar{u}(x) \in M_{g^{t-l}}\right\}$$

are stable under x-multiplication.

5.1 Characterization of elements of $M_{g^l}^q$

We now give a corollary of Lemma 11.

Corollary 14 *The element $f(x) \in \mathcal{R}_{g^t}^q$ is invertible if and only if $f_0(x) \neq 0$.*

The finite group $M_{g^l}^q$ is the multiplicative group of the ring $\mathcal{R}_{g^l}^q$. It is a finite abelian group and therefore can be expressed as a product of cyclic groups. We investigate this structure.

Let us distinguish between two cases: If $l = 1$ the ring $\mathcal{R}_q^q$ is a finite field; hence its multiplicative group is cyclic. If $g(x)$ is a primitive polynomial, i.e. if $\mathrm{ord}(g(x)) = q^r - 1$ then $x \in M_g^q$ is a generator. In either case, we denote by $h(x) \in M_g^q$ a generator of the cyclic group.

Let us now consider the case $l \geq 2$.

Theorem 15 *The order of the group $M_{g^l}^q$ is $(q^r - 1)q^{(l-1)r}$. Moreover*

$$M_{g^l}^q \cong M_g^q \times S_p,$$

where S_p is the p-Sylow subgroup of $M_{g^l}^q$.

We now study the structure of the p-Sylow subgroup.

Proposition 16 *Let $f \in M_{g^l}^q$. The multiplicative order of f is a power of p if and only if there exists a polynomial $m(x) \in \mathbb{F}_q[x]$ such that*

$$f(x) = 1 + m(x)g(x).$$

Proof

$$\begin{aligned} \mathrm{ord}(f(x)) \text{ is a power of } p &\iff f(x)^{p^k} = 1 \text{ for } k \gg 0 \\ &\iff f(x) \equiv 1 \pmod{g(x)} \end{aligned}$$

where the last equivalence follows from writing $f(x) = 1 + m(x)g(x)$ and raising both sides to the p^k-th power. □

Notations Let $\alpha \in \mathbb{F}_q$ be an algebraic element of degree δ over $\mathbb{F}_p$. Therefore $\mathbb{F}_q = \mathbb{F}_p[\alpha]$. Let

$$a_{i,j,k}(x) = 1 + \alpha^i x^j g(x)^k \in S_p, \tag{4}$$

where $0 \leq i < \delta$, $0 \leq j < r$, $1 \leq k < l$.

Lemma 17 *For any polynomial of the form*

$$f(x) = 1 + f_k(x)g(x)^k + m(x)g(x)^{k+1} \in \mathbb{F}_q[x]$$

with $k \in \mathbb{N}_+$ *and* $\deg f_k(x) < \deg g(x)$*, there exist*

$$c_{(i,j)} \in \{0, 1, \ldots, p-1\}$$

such that

$$\prod_{i,j} a_{i,j,k}(x)^{c_{(i,j)}} \equiv f(x) \pmod{g(x)^{k+1}}$$

for every $0 \leq i < \delta$ *and* $0 \leq j < r$.

Proof Let us suppose that $p \nmid k$. The polynomial $f_k(x)$ can be written as

$$f_k(x) = \sum_{i,j} c_{(ij)} \alpha^i x^j,$$

with $c_{(ij)} \in \mathbb{F}_p$. It follows that

$$\begin{aligned} \prod_{i,j} a_{i,j,k}(x)^{c_{(ij)}} &= 1 + \sum_{i,j} c_{(ij)} \alpha^i x^j g(x)^k + m'(x)g(x)^{k+1} \\ &\equiv f(x) \pmod{g(x)^{k+1}}. \end{aligned}$$

The case $p \mid k$ is analogous. It starts by setting $h = ph'$ and continues as above. □

Theorem 18 *Let* S_p *be the* p*-Sylow subgroup of* $M^q_{g^l}$*. Then*

$$S_p \cong \prod_{i,j,k} \big(a_{i,j,k}(x)\big),$$

where $\big(a_{i,j,k}(x)\big) \subset S_p$ *is the cyclic group generated by* $a_{i,j,k}(x)$ *and the parameter* k *satisfies the condition* $p \nmid k$.

Proof The polynomial $f_1(x)$ can be expressed as

$$f_1(x) = \sum_{i,j} c_{(ij1)} \alpha^i x^j.$$

From the previous lemma we have

$$\prod_{i,j} a_{i,j,1}(x)^{c_{(ij1)}} = 1 + f_1(x)g(x) + m(x)g(x)^2. \tag{5}$$

Let now consider $\tilde{f}_2(x) \equiv f_2(x) - m(x) \pmod{g(x)}$; then

$$\tilde{f}_2(x) = \sum_{i,j} c_{(ij2)} \alpha^i x^j.$$

Using the lemma once more, we obtain

$$\prod_{i,j} a_{i,j,2}(x)^{c_{(ij2)}} = 1 + \tilde{f}_2(x) g(x)^2 + \tilde{m}(x) g(x)^4. \tag{6}$$

Multiplying the relations (5) and (6):

$$\begin{aligned}&(1 + f_1(x)g(x) + m(x)g(x)^2)(1 + \tilde{f}_2(x)g(x)^2 + \tilde{m}(x)g(x)^4)\\ &= 1 + f_1(x)g(x) + f_2(x)g(x)^2 + \hat{m}(x)g(x)^3.\end{aligned}$$

The claim is obtained by iterating this computation l times. □

Let us now consider the homomorphism of groups

$$\mu : \prod_{i,j,k} \left(a_{i,j,k}(x)\right) \to S_p,$$

Theorem 19 *The following holds*:

$$\prod_{i,j,k} a_{i,j,k}(x)^{c_{(ijk)}} \equiv 1 \pmod{g(x)^l} \iff c_{(ijk)} \equiv 0 \pmod{\operatorname{ord}(a_{i,j,k}(x))}.$$

Proof Since

$$c_{(ijk)} = p^{s_{(ijk)}} c'_{(ijk)},$$

it follows that

$$a_{i,j,k}(x)^{c_{(ijk)}} = 1 + \sum_{h=1}^{c'_{(ijk)}} \binom{c'_{(ijk)}}{h} \left(\alpha^{ip^{s_{(ijk)}}} x^{jp^{s_{(ijk)}}} g(x)^{kp^{s_{(ijk)}}}\right)^h. \tag{7}$$

Let $\mathfrak{K}p^{\mathfrak{s}} := \min_{i,j,k} kp^{s_{(ijk)}}$. In order to use this notation it is important that $p \nmid k$, so that any triplet $(\bar{i}, \bar{j}, \bar{k})$ giving this minimum is such that $s_{(\bar{i}\bar{j}\bar{k})} = \mathfrak{s}$.

Sorting all monomials in (7) according to the power of $g(x)$ that they contain, we obtain

$$m_{\mathfrak{K}p^{\mathfrak{s}}}(x) := \sum_{(i,j)\in\mathcal{J}} c'_{(ijk)} \alpha^{ip^{\mathfrak{s}}} x^{jp^{\mathfrak{s}}} = \left(\sum_{(i,j)\in\mathcal{J}} c'_{(ijk)} \alpha^i x^j\right)^{p^{\mathfrak{s}}}$$

where $\mathcal{J}$ is the set of all pairs (i, j) for which the exponent $kp^{s_{(ijk)}}$ is minimal.

The polynomial $m'(x) := \sum_{(i,j)\in\mathcal{J}} c'_{(ijk)}\alpha^i x^j$ does not vanish, because the pairs (i, j) appear exactly once in the sum. Moreover, the condition $j < \deg g(x)$ implies that no factor of $g(x)$ divides $m'(x)$. The hypothesis is then satisfied if and only if $\mathfrak{K}p^5 \geq l$.

This last remark concludes the proof, because for every factor of the product

$$a_{i,j,k}(x)^{c_{(ijk)}} \equiv 1 \pmod{g(x)^l},$$

hence $c_{(ijk)} \equiv 0 \pmod{\operatorname{ord}(a_{i,j,k}(x))}$. □

5.2 Set of generators of the x-orbits of $M^q_{g^l}$

Theorem 20 *The elements $a_{i,j,k}(x) \in M^q_{g^l}$ have order*

$$\operatorname{ord}(a_{i,j,k}(x)) = p^{\lceil \log_p l/k \rceil}.$$

Proof Thanks to Theorem 16, the order of the elements $a_{i,j,k}(x)$ is a power of p. Since $\gcd(\alpha^i x^j, g(x)) = 1$ we get

$$(\alpha^i x^j g(x)^k)^{p^m} \equiv 0 \pmod{g(x)^l} \iff kp^m \geq l.$$

From the definition of order it follows that $m = \lceil \log_p l/k \rceil$. □

To investigate the construction of the x-orbits more in depth, we divide the cyclic group (x) into a product of other cyclic groups.

Theorem 21 *The order of the element $x \in M^q_{g^l}$ is*

$$\operatorname{ord}(x) = \operatorname{ord}(g(x)) \cdot p^{\lceil \log_p l \rceil}.$$

Corollary 22 *The cyclic group* (x) $\subset M^q_{g^l}$ *is isomorphic to the product of two cyclic groups whose orders are* $p^{\lceil \log_p l \rceil}$ *and* $\operatorname{ord}(g(x))$.

Remark 3 Using the representation of the groups $M^q_{g^l}$ given in the previous section we can make the previous corollary explicit. We have

$$(\mathrm{x}) \cong \left(\mathrm{x}_p(\mathrm{x})\right) \times \left(\mathrm{x}_{o_g}(\mathrm{x})\right)$$

where $\left(\mathrm{x}_p(x)\right) \subset S_p$ and $\left(\mathrm{x}_p(x)\right) \subset M^q_g$. Without loss of generality let

$$\mathrm{x}_p(x) := x^{\operatorname{ord}(g(x))} \in S_p \text{ and } \mathrm{x}_{o_g}(x) := h(x)^{\frac{q^r-1}{\operatorname{ord}(g(x))}} \in M^q_g$$

where $h(x)$ is a generator of M^q_q.

Theorem 23 *Let* $\mathrm{x}_p(x) \in S_p \subset M_{g^l}^q$ *be an element of order* $p^{\lceil \log_p l \rceil}$. *There exist parameters* $0 \leq i_0 < \delta - 1$ *and* $0 \leq j_0 < \deg g(x)$ *such that*

$$S_p \cong \left(\mathrm{x}_p(x)\right) \times \prod_{\substack{i,\, j,\, k \\ (i.j.k) \neq (i_0,\, j_0,\, 1)}} \left(a_{i,j,k}(x)\right).$$

Proof Since $\mathrm{x}_p(x) \in S_p$, then

$$\mathrm{x}_p(x) \equiv \prod_{i,j,k} a_{i,j,k}(x)^{c_{(ijk)}} \pmod{g(x)^l}.$$

The order of the element is $p^{\lceil \log_p l \rceil}$. Then there exist $0 \leq i_0 < \delta - 1$ and $0 \leq j_0 < \deg g(x)$ such that

$$\gcd(c_{(i_0 j_0 1)},\, p) = 1.$$

For every $e_{(ijk)} \in \mathbb{N}$

$$\prod_{i,j,k} a_{i,j,k}(x)^{e_{(ijk)}} = \mathrm{x}_p(x)^{\tilde{e}_p} \cdot \prod_{\substack{i,\, j,\, k \\ (i,\, j,\, k) \neq (i_0,\, j_0,\, 1)}} a_{i,j,k}(x)^{\tilde{e}_{(ijk)}},$$

with

$$\begin{aligned} \tilde{e}_p &\equiv e_{(i_0 j_0 1)} \cdot (c_{(i_0 j_0 1)})^{-1} \left(\mathrm{mod}\, p^{\lceil \log_p l \rceil}\right) \\ \tilde{e}_{(ijk)} &\equiv e_{(ijk)} - c_{(ijk)} \tilde{e}_p \left(\mathrm{mod}\, p^{\lceil \log_p l/k \rceil}\right). \end{aligned}$$

□

We can now characterize every possible representative of the x-orbits of $M_{g^l}^q$.

Theorem 24 *Let* $g(x) \in \mathbb{F}_q[x]$ *be an irreducible polynomial of degree* r *and let* $l \geq 2$. *There exist* $0 \leq i_0 < \delta - 1$ *and* $0 \leq j_0 < \deg g(x)$ *such that the set*

$$\left\{ h(x)^m \cdot \prod_{\substack{(i,\, j,\, k) \neq (i_0,\, j_0,\, 1) \\ 0 \leq i < \delta,\ 0 \leq j < r \\ 1 \leq k \leq t,\ p \nmid k}} (1 + \alpha^i x^j g(x)^k)^{c_{(ijk)}} \pmod{g(x)^l} \right\},$$

is a family of representatives of the orbits in $M_{g^l}^q$. *Here,* $h(x)$ *is a primitive element of* $\mathcal{R}_g^q$, $\alpha \in \mathbb{F}_q$ *is an algebraic element of degree* δ *over* $\mathbb{F}_p$, *and* m *and* $c_{(ijk)}$ *are such that* $0 \leq m < \frac{q^r - 1}{\mathrm{ord}(g(x))}$ *and* $0 \leq c_{(ijk)} \leq p^{\lceil \log_p l/k \rceil}$.

6 Pseudocode of the algorithm

input : $g(x) \in \mathbb{F}_q[x]$: generator polynomial of the CRC code;
$n \in \mathbb{N}$: length of the code ($n < q^{\deg g(x)} - 1$).
output : $\{A_0, A_1, \ldots, A_n\}$: weight distribution of the dual code.

Step 1 - *Factorization of $g(x)$ and computation of the orders.*
$g(x) = \prod_{l=1}^{m} g_l(x)^{e_l}$; $o_{g_l} := \mathrm{ord}(g_l(x))$ and $o_g := \mathrm{ord}(g(x))$.
Step 2 - *Representatives $\mathcal{R}_g^q$.*
for $l \leftarrow 1$ ***to*** m **do**
$h(x)$ the generator of the cyclic group $M_{g_l}^q$.
Step 2.1 - *Representatives of $M_{g_l}^q$*
case $g_l(x)$ *primitive:* the polynomial x is the representative.
case $g_l(x)$ *not primitive:* the set of representatives is
$\{h(x)^k \pmod{g_l(x)} \mid 0 \le k < \frac{q^{\deg g_l(x)}-1}{o_{g_l}}\}$.
Step 2.2 - *Representatives of $\mathcal{R}_{g_l^{e_l}}^q$*
for $r \leftarrow 2$ ***to*** e_l **do**
Step 2.2.1 - *Generators of S_p*
for $\alpha \in \mathbb{F}_q$ algebraic of degree δ over $\mathbb{F}_p$, the set of generators is
$\left\{a_{i,j,k}(x) := 1 + \alpha^i x^j g_l(x)^k\right\}$.
Step 2.2.2 - *Representatives of $M_{g_l^r}^q$*
$\mathrm{x}_p(x) := x^{q^{\deg g_l(x)}-1} \pmod{g_l(x)^2} = 1 + f(x)g_l(x)$ with $f(x) = \sum \alpha^i x^j$. Pick indices i_0, j_0 from the monomials of $f(x)$.
The representatives are

$$u_{ijkm}(x) := h(x)^m \prod_{\substack{i,\,j,\,k \\ (i.j.k) \neq (i_0,\,j_0,\,1)}} a_{i,j,k}(x)^{c_{ijk}} \pmod{g_l(x)^r}.$$

Step 2.2.3 - *Representatives of $\mathcal{R}_{g_l^{e_l}}^q$*
$\left\{u_{ijkm}(x) g_l(x)^{e_l - r}\right\}$ is a subset of the representatives of the ring.
Step 2.3 - *Representatives of $\mathcal{R}_g^q$*
Apply Theorem 3.
Step 3 - *Fundamental Step*
Apply section 3 to all the representatives of *Step 2.4*.

6.1 Example

Let consider $F_4 = \mathbb{F}_2[\alpha]$ with $\alpha \in \mathbb{F}_4$ such that $\alpha^2 + \alpha + 1 = 0$. We apply the first two steps of the algorithm to the ring $\mathcal{R}_{g^2}^4$ where $g(x) = x^2 + x + \alpha$.

We know that $\mathcal{R}_{g^2}^4 = \{0\} \sqcup g(x)M_g^4 \sqcup M_{g^2}^4$.

Let us first compute the representatives of $g(x)M_g^4$. The order of $g(x)$ is 5. A generator of M_g^4 is $h(x) := x + \alpha$. The set of representatives are then

$$O_{gM_g^4} = \left\{g(x)h(x),\, g(x)h(x)^2,\, g(x)h(x)^3\right\}.$$

We now consider the set $M^4_{g^2}$. The generators of S_p are:

$$\{a_{0,0,1}(x), a_{1,0,1}(x), a_{0,1,1}(x), a_{1,1,1}(x)\}.$$

Since $\mathrm{x}_p(x) = x^{4^2-1} \equiv 1 + (\alpha x + x)g(x) \pmod{g(x)^2}$, we decide not to consider in the computation of the representatives the polynomial corresponding to $i_0 = 1$ and $j_0 = 1$, i.e. $a_{1,1,1}(x) = 1 + \alpha x g(x)$.

It follows that the representatives of the set are the elements of the union of the following three sets:

$$\begin{aligned} O^i_{M^4_{g^2}} = \{&h(x)^i, h(x)^i a_{0,0,1}(x), h(x)^i a_{1,0,1}(x), h(x)^i a_{0,1,1}(x), \\ &h(x)^i a_{0,0,1}(x) a_{1,0,1}(x), h(x)^i a_{0,0,1}(x) a_{0,1,1}(x), h(x)^i a_{1,0,1}(x) a_{0,1,1}(x), \\ &h(x)^i a_{0,0,1}(x) a_{1,0,1}(x) a_{0,1,1}(x)\}, \end{aligned}$$

with $i = 1, 2, 3$.

A complete set of representatives of the ring $\mathcal{R}^4_{g^2}$ is then

$$O_{\mathcal{R}^4_{g^2}} = O_{gM^4_g} \cup \bigcup_{i=1}^{3} O^i_{M^4_{g^2}}.$$

7 Complexity

The complexity was investigated with the help of M.J. Gatto of the Institute of Theoretical Computer Science of the ETH Zürich.

We consider only the case of a ring obtained as a quotient by the power of an irreducible polynomial. The general case follows directly. Recall that $g(x)$ is an irreducible polynomial and $\deg g(x) = r$.

Since the complexity of Steps 1 and 2 of the algorithm is negligible with respect to the complexity of Step 3, we focus on the last step.

1. *Complexity of relation* (2).
   To completely determine the LRS, starting from a representative element (namely $u(x)$), we need to compute rt times the relation (2). The cost of this operation is:
   - $xu(x)$ is a constant time operation,
   - $u_{rt-1}g(x)$ are at most rt multiplications that are of constant time complexity, it costs $\mathcal{O}(rt)$
   - $xu(x) - u_{rt-1}g(x)$ requires at most rt subtractions, therefore it costs $\mathcal{O}(rt)$.

   Thus the complexity is $\mathcal{O}(r^2t^2)$.
2. *Computation of the weight of the first codeword*
   Without any excessive use of memory and starting from the first tr entries, is it possible to compute the remaining entries of the codeword in constant time. Therefore the complexity is $\mathcal{O}(n)$.
3. *Computation of the weight of any other codeword from the LRS*

The cost of constructing the entries of the LRS is constant. From Lemma 7 we have $|C_u^{\perp}| = \operatorname{ord}\left(\frac{g(x)}{\gcd(g(x),u(x))}\right)$. Since $g(x)$ is primitive,

$$\operatorname{ord}\left(\frac{g(x)^t}{\gcd(g(x)^t, u(x))}\right) \leq \operatorname{ord}(g(x)^t) = \operatorname{ord}(g(x))\, p^{\lceil \log_p t \rceil} \leq (p^{\delta r} - 1)\, p^{\lceil \log_p t \rceil}.$$

It follows that the cost is

$$\mathcal{O}\left((p^{\delta r} - 1)\, p^{\lceil \log_p t \rceil}\right) = \mathcal{O}(t p^{\delta r}).$$

The complexity of the algorithm is the complexity of Step 3 times the number of representatives of the ring.

Following the conditions of Theorem 24 it is easy to show that $p^{\delta r} r t^2 \delta$ is an upper bound on the number of the representatives.

Therefore the overall complexity of the algorithm is

$$\mathcal{O}\left((p^{\delta r} r t^2 \delta)(r^2 t^2 + n + t p^{\delta r})\right) = \mathcal{O}\left((p^{\delta r} r t^2 \delta)(n + t p^{\delta r})\right),$$

since $r^2 t^2$ is negligible with respect to n.

Acknowledgments This work is a part of the author's master thesis [5] which was written under the direction of Patrizia Gianni and Barry M. Trager. The author wishes to express his gratitude for their guidance during this work. He is also thankful to the organizers of the workshop "Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics" for the opportunity to present part of this work.

References

1. Castagnoli, G., Bräuer, S., Hermann, M.: Optimization of cyclic redundancy check codes with 24 and 32 parity check bits. IEEE Trans. Commun. **41**(6), 535–892 (1993)
2. Fujiwara, T., Kasami, T., Lin, A.S.: Error detecting capabilities of the shortened hamming codes adopted for error detection in ieee standard 802.3. IEEE Trans. Commun. **37**(9), 986–989 (1989)
3. Kronecker, L.: Zur theorie der elimination einer variabeln aus zwei algebraischen gleichungen. Monatsberichte der Königlich Preussischen Akademie der Wissenschaften, pp. 535–600 (1881)
4. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1994)
5. Manganiello, F.: Calcolo della distribuzione dei pesi nei codici ciclici accorciati (in italian). Master's thesis, Universitá di Pisa, Italy. http://etd.adm.unipi.it/theses/available/etd-09292005-190538 (2005)
6. MacWilliams, F.J., Sloane, N.J.A.: The theory of error-correcting codes. North-Holland, Amsterdam (1977)
7. Sala, M.: A groebner bases technique to compute distance and weight distribution of cyclic codes and their shortened codes. J. Algebra. Appl. **6**(3), 403–414 (2007)
8. Wicker, S.B.: Error control systems for digital communication and storage. Prentice Hall, New Jersey (1995)